REGULATIONS FOR THE DESTRUCTION OF RECORDS CONTAINING SOCIAL SECURITY NUMBERS

Purpose

These new regulations are needed to curb the growing problem of identity theft. Identity theft occurs when a criminal uses another person's personal information to take on that person's identity. The intent of these regulations is to protect individuals from identity theft by eliminating unauthorized access to social security numbers in public records.

Basis

The authority to promulgate these regulations can be found in the § 42.1-82. of the *Code of Virginia* (1950) as amended. The *Code* grants to the Board the authority to issue regulations establishing procedures for the disposal, physical destruction or other disposition of public records containing social security numbers. These regulations shall include all reasonable steps to destroy such documents by (i) shredding, (ii) erasing, (iii) pulping, (iv) disintegration, (v) incineration or (vi) otherwise modifying the social security numbers in those records to make them unreadable or undecipherable by any means.

Substance

The following are new requirements added to reflect changes made to §42.1-82.1.

Definitions:

Electronic Record – Records created or stored by electronic means, including but not limited to, computer files and optically scanned files on tapes, disks, cd-roms or internal memory.

Erasure – To remove electronic information so that it cannot be retrieved from the media on which the information is stored.

Redaction – The process of editing existing printed documents to delete or obliterate selected information.

Shredding – A means of destroying paper records by mechanical cutting. Straight cut shredders cut in one direction only, cross cut shredders cut in two directions, 90 degrees from the other.

Purpose:

The custodian of public records is obligated to protect social security numbers that may be contained in public records to prevent the misuse of personal information. Any public records, regardless of media, that contain social security numbers are to be destroyed in a manner that protects the confidentiality of the information. These records are to be destroyed, made undecipherable or erased so as to make the social security numbers unreadable by any means.

Procedures:

A. Paper Records – There are several accepted methods to destroy paper records containing social security numbers. The method used is determined by the volume of records that need to be destroyed, as well as availability of resources and funds. Care must be taken to ensure that until the records are destroyed they are protected from accidental or unapproved access.

The acceptable methods of hardcopy records destruction are as follows:

1. Shredding - Shredding involves the use of a mechanical cutter to cut the paper in such a way as to render the document unreadable. There are two forms of shredders:

a. Strip shredders that reduce sheets of paper into thin strips that when mixed with other shreds cannot be easily recreated into the original document. The strips shall not exceed $3/8^{th}$ inches in width. A recommended practice is to feed documents in to the shredder so that the document text is perpendicular, rather than parallel, to the shredding mechanism. This reduces the possibility of a full line of text being on single strip of shredded paper.

b. Cross-cut shredders that use two sets of cutters set at right angles to each which reduces the paper to a confetti-like substance. This provides maximum protection for privacy protected documents.

2. Use of a Commercial Shredder - Commercial shredders must be either of the two acceptable types outlined above.

Whether you have the shredding done onsite or offsite a certificate of destruction which lists what records have been destroyed, the date of destruction and who did the shredding is required.

If the shredding is done offsite, locked bins or other forms of secure storage are required to protect the records before they are shredded. The company doing the shredding must be bonded. The agency contracting for the shredding must determine how long after the bins are picked up the contents are shredded and require that the bins are secured until they are shredded. It is the agencies' responsibility to protect the social security numbers on the records they handle.

As indicated earlier, there are other methods for disposing of records such as:

1. Pulping – Paper is macerated, mixed with water and turned into mash of paper fibers and liquid.

2. Incineration – Placing the paper into a furnace and destroying them completely by burning.

B. Electronic Records - Unlike a paper record where you can visibly determine if the document is unreadable, electronic records require special handling to make information unreadable. Merely using the delete key does not actually delete the file, only the pointer to that file is

deleted. Easily available off the shelf programs can re-index the file allowing it to be opened and read. The decentralization of computer based information also results in information being stored on multiple computers, on back-up tapes and portable media. In addition to discrete electronic documents, social security numbers may also be contained as a field(s) in databases or other files. In such cases, the issue is removing the data contained within a field as well as the disposition of the entire file.

Processes to protect and destroy social security numbers in electronic format and stored on information or record-keeping systems must be established.

1. Security – Access to information containing social security information must be restricted to those with a need to know or use. Security parameters of information systems must be established to restrict access to data to only the employees who legitimately work with this information. If the information system is connected to the Internet, it must be protected by a firewall, at a minimum and with encryption, secure socket layer (SSL) preferred.

2. Control – Limit the number of places where social security numbers are stored in info systems, and limit the locations within each system. Limit the amount of information that is retained on local computers; identify back-up tapes and what is done with them. If tapes, CDs or other removable media are used to store information containing social security numbers, the removable media must be retained in a secure location.

3. Records Retention – Determine if the social security numbers are required as part of the records series. If not, do not retain this data. Determine if the records are covered by a records retention schedule and that the retention schedules are being followed.

4. Destruction – When the records retention period has expired and the information needs to be destroyed, choose an appropriate method to protect the social security numbers.

a. Files on a personal computer require that the information is not only deleted but also overwritten to prevent the information from being reconstructed. "Shredder" programs are available that overwrite the data with meaningless data multiple times to totally obliterate the original data.

b. Back-up tapes should be overwritten at the earliest possible time. These tapes should not be held longer than the retention period for the information retained on them.

c. Floppy disks, tapes and other magnetic storage devices must also have the data on them overwritten to protect the social security numbers stored on them. These materials can be shredded in a shredder to insure that the information is totally destroyed–they may be exposed to a powerful magnetic field several times to disrupt the information stored on them or they could be incinerated. If magnetic media is used, the data must be reviewed to ensure that the social security numbers are not retrievable

d. CD-ROMs should be physically broken, into several pieces, to be rendered unusable. If possible they should be shredded.

e. When disposing of computers that contain social security numbers or other privacy protected information, care should be taken to protect the information that was stored in them. The hard drives should be wiped clean and inspected to make sure no privacy protected data remains. It may be necessary to remove the hard drive and dispose of it separately. Alternatively, the system can be programmed to change all social security numbers to 999-99-9999 before deleting files to make the data useless even if the file is captured.

C. Redaction -To redact is to edit existing documents, either hard copy or electronic, to remove or make irretrievable the social security number information. Redaction is the process of making specific parts of a document illegible. Here it is being applied to social security number data elements.

1. Hard Copy Records – Hard copy redaction involves using opaque material to mask off or obliterate the protected information. A permanent ink marker or similar material can be used to mark out (preferably on a copy, so the information isn't lost) the information so that it cannot be viewed by those not permitted access to it. The image may have to be marked out on both sides of the document to prevent image bleed through or the redacted copy can be copied again – the second copy is more secure because the social security number never appeared on that version of the record but all other information is still available.

2. Electronic Documents –Commercial off the shelf redaction programs are available to accomplish electronically what is done physically with hard copy documents. These programs allow you to provide access to redacted documents while retaining un-redacted electronic documents to authorized individuals; this is acceptable as long as only authorized persons have access to the un-redacted information.

Alternatives

There currently is no viable method for preventing access to social security numbers other than the removal of social security numbers from public records.

Family Impact Statement

This regulation will have no impact on the institution of the family or on family stability.